Fecha de recepción: 31 de agosto de 2016 / Fecha de aprobación: 04 de octubre de 2017

Revista de Derecho Comunicaciones y Nuevas Tecnologías

DATOS EMPRESARIOS, PROTECCIÓN EN LA ACTUAL SOCIEDAD DE LA INFORMACIÓN: UNA VISIÓN ARGENTINA

MARÍA EUGENIA LO GIUDICE

Artículo de reflexión

DOI: http://dx.doi.org/10.15425/redecom.17.2017.06

Universidad de los Andes
Facultad de Derecho
Rev. derecho comun. nuevas tecnol. No. 17
enero - junio de 2017. e-ISSN 1909-7786

Datos empresarios, protección en la actual sociedad de la información: una visión argentina

Resumen

Consciente de los beneficios que genera la actual relación sociedad-tecnologías-derecho, también se resaltó la presencia de amenazas y vulnerabilidades ante las nuevas conductas generadas en este contexto. Se señaló el imperioso manejo responsable de la información dentro de la empresa.

Se sustanció un proceso analítico descriptivo, enfocado en el marco jurídico normativo de Argentina y la Convención de Budapest sobre ciberdelincuencia (Council of Europe, 2001).

Se expusieron técnicas utilizadas en amenazas informáticas para obtener de forma no autorizada información, provocando fuga de datos, citándose casos ejemplificadores reconocidos en el ámbito público.

La conclusión a que se arribó fue la necesidad de precisar el concepto de *ingeniería social*, como contrapuesto al de *ingeniería informática*. En este sentido se observó la imperiosa necesidad de pensar y proponer estrategias suficientes desde el punto de vista legal, para anticiparse a la eventual generación de situaciones críticas, evitando posibles riesgos ocultos.

Palabras clave: sociedad del conocimiento, datos, nuevas tecnologías, seguridad de la información, delitos informáticos, ingeniería social, empresa.

Business data, its protection in the current knowledge society: an argentine perspective

Abstract

Aware of the benefits generated by the current relationship, society-technologies- law, It was noted threats and vulnerabilities to the new behaviors generated in this context. Highlighting the legal responsibility for information management within the companies.

It describes an analytical process centered on the regulatory legal framework of Argentina and the Budapest Convention on Cybercrime.

This report present some techniques used as threats to obtain unauthorized information, causing data loss and some typical cases recognized at the public level.

It is important to note that the concept of “social engineering” and “computer engineering” should be clarified. Due to what is exposed there is an urgent claim to think and propose adequate strategies from the legal point of view, to strengthen the problems generated by avoiding the potential risks.

Keywords: Knowledge society, information and communications technology, security management information, cybercrime, social engineering threats, enterprise.

Datos empresarios, protección en la actual sociedad de la información: una visión argentina*

MARÍA EUGENIA LO GIUDICE**

SUMARIO

* Cómo citar este artículo: Lo Giudice, M. E. (Junio, 2017). Datos empresarios, protección en la actual sociedad de la información: una visión argentina. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* (17). Universidad de los Andes (Colombia). http://dx.doi.org/10.15425/redecom.17.2017.06

Resultado de la investigación en el marco de actividad de ciencia y técnica "Espionaje comercial con robo de información confidencial" ACyT AS1420, financiado por el Instituto de Ciencias Sociales y Disciplinas Proyectuales (INSOD), Universidad Argentina de la Empresa. En tal investigación colaboraron: el abogado especialista en derecho de alta tecnología Luciano Galmarini y el licenciado en sistemas Omar Cuarterolo.

** Abogada, Universidad Nacional de Buenos Aires. Especialista en derecho de alta tecnología, Pontificia Universidad Católica Argentina, Santa María de los Buenos Aires. Doctoranda, Universidad Nacional de Buenos Aires. Docente adjunta e investigadora en la Universidad Argentina de la Empresa. Buenos Aires, Argentina. Correo: eugenialogiudice@gmail.com

Introducción

Actualmente es indiscutible el rol central que cumple la tecnología en la vida cotidiana. Pero asimismo el hecho tecnológico genera frecuentemente una cierta sensación de riesgo, entendido este como aquello a lo que se está expuesto, y que si no se lo tiene en cuenta puede presentarse en cualquier momento generando algún efecto negativo, y por lo tanto se le debe prever e intervenir con anticipación. Al decir del sociólogo alemán Beck (2004), quien se ocupó de los problemas de la sociedad moderna, "los riesgos creídos como tales, son la fusta con la que se puede hacer que el caballo del presente venga al galope" (p. 193).

Las tecnologías de la información y la comunicación (TIC) arrojan beneficios numerosos, aunque también su influencia negativa se hace presente y no por esto se debe satanizar su uso. Por ellas se han definido nuevos conceptos en numerosos campos como el de la salud, por su influencia en el cuerpo y la mente del ser humano.

En su aspecto positivo se señala permanentemente la contribución de las TIC a la ciencia y a la sociedad en general. En la visión negativa, para plasmar algunos ejemplos desde el punto de vista de la psicología, se incorporaron neologismos como *phubbing,* que proviene de la sumatoria de los términos en inglés *phone* y *snubbing,* y refiere al acto de ignorar a alguien por mirar el teléfono móvil; también *nomofobia,* del mismo origen, que significa *no mobile phone*, es decir, miedo a estar sin el teléfono móvil. Aplicado a los seres vivos en general, en otros campos como el fisiológico, las TIC han contribuido ampliamente, pero asimismo sería extenso listar los diversos desórdenes provocados por ellas: los efectos nocivos de los químicos usados en tecnología, la aparición de síndromes en el ser humano como el del túnel carpiano, sordera, obesidad o desastres naturales ocasionados por el uso de elementos tecnológicos, por ejemplo.

Se evidencia una etapa de transformación de la sociedad, una sensación de incertidumbre provocada por el efecto de estas nuevas tecnologías, ante lo impredecible percibido a veces como una amenaza. Se plantean así en el mundo del derecho conceptos nuevos como el principio de orden público tecnológico o el principio de equivalencia funcional o el principio de neutralidad tecnológica.

Actualmente y a través del uso de las tecnologías se ha pasado del conocido estadio de la sociedad de la información —aquella que surgió ante la facilidad de acceso a datos mediante la tecnología— a otro nivel más avanzado, cual es el de la sociedad del conocimiento. En la sociedad del conocimiento ya no constituye una novedad la facilidad en la obtención de los datos, sino lo importante es que se comprenda el valor asignado a esa sumatoria de información, es decir, al dato en sí mismo. El desarrollo tanto en lo económico como en lo social se basa en ellos, entendiéndose por dato la unidad mínima de información.

El uso de la tecnología al servicio de la vida cotidiana hace que los datos queden resguar-

dados en servidores propios o en servidores remotos, lo cual genera cierto riesgo, que es lo que caracteriza a nuestra propia y actual cultura, la cual siguiendo al sociólogo Luhmann ha sido definida por autores como Acevedo y Vargas (2000), como *sociedad del riesgo*.

I. EL RIESGO Y LA INFORMACIÓN EN LA ACTUAL SOCIEDAD

Se cuestiona por qué o cómo vinculamos el "riesgo" a la "información" para comprender el estereotipo de sociedad del riesgo que se transita en la actualidad.

Así, se debe resaltar la importancia que le cabe al tratamiento de los datos, porque de ello derivará la responsabilidad que recae sobre los sujetos de derechos, sean estos tanto personas físicas o naturales como personas jurídicas. Es decir, involucra el sujeto físico individual y los sujetos de existencia ideales, entendidos como aquellos entes con capacidad para adquirir derechos y contraer obligaciones, que no sean una persona física, esto es, empresas, organizaciones estatales y no gubernamentales, etc.

De acuerdo a recientes informes estadísticos requeridos por el Departamento para Negocios, Innovaciones y Habilidades del Gobierno de Gran Bretaña (HM Council Government, 2015), el 81 % de las grandes organizaciones apuntaron a que los propios empleados se han visto envueltos en violaciones a la información, ¿no será pues hora de que se considere al comportamiento de quienes forman parte de ellas como un factor posible de riesgo en determinadas circunstancias?

II. SITUACIÓN ACTUAL EN LA LEGISLACIÓN ARGENTINA

Respecto a los datos y su correcto tratamiento, la República Argentina se enmarca legalmente en su Carta Magna o Constitución Nacional de 1994 y en legislación específica como la Ley de protección de los datos personales (L. 25326/2000), el decreto que la reglamenta (D. 1558/2011) y la Ley de confidencialidad (L. 24766/1996).

La Ley de protección de los datos personales se aplica también a los datos de las personas de existencia ideal. Se hace explícita referencia a la información sometida al tratamiento o procesamiento electrónico o automatizado de los datos, tomando en consideración: los datos en sí mismos, la infraestructura para su tratamiento y el componente humano involucrado en su procesamiento.

De acuerdo con el artículo 2 de dicha ley, por datos personales se entiende cualquier información que se refiera a las personas, ya sean de existencia natural o de existencia ideal, incluso que puedan ser determinables a futuro si no lo están expresamente determinadas en un momento específico.

En cuanto a la infraestructura para el tratamiento de los datos, se protege tanto al dato, considerado como la unidad mínima de infor-

mación, como a los conjuntos organizados de datos personales, pudiendo tratarse de archivos, registros, bases o bancos de datos. Lo que se protege es el objeto de tratamiento en sus diferentes formas (electrónico o no), así como cualquier tipo de modalidad de "formación, almacenamiento, organización o acceso" (art. 2).

Focalizando el elemento humano, la ley en comento atribuye determinadas responsabilidades. Se refiere a las que le caben, por un lado, a los titulares de las diferentes disposiciones en que están resguardados o almacenados los datos, ya sean registros, archivos, bases de datos, etc. y, por otro lado, a los propios usuarios de esos datos.

Asimismo, tales sujetos responsables deben preservar las garantías de seguridad, integridad y confidencialidad de los datos, "ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado" (art. 2).

III. LA ACCIÓN HUMANA

En este orden de ideas, se propone identificar posibles vulnerabilidades desde el punto de vista del riesgo originado en la acción humana. Se hace referencia a conductas que podrían surgir del hecho ajeno a la empresa, como de acciones propias internas, categorizándose de acuerdo a lo que se entiende en el campo jurídico como culpa, negligencia o impericia en el obrar.

Se pueden diferenciar tres aspectos en donde la acción humana se ve involucrada. En lo referido a lo humano propiamente dicho, se puntualiza la relación con las conductas de las personas. En lo que concierne a lo físico, se tienen en cuenta amenazas que incumben a lo humano y a lo natural. En cuanto a lo tecnológico, aspectos que intervienen en la estructura misma del sistema, que a su vez pueden influir tanto en lo humano como en lo físico.

En la Ley 25326/2000 se señalan ciertas categorías y frente a ellas se exigen diversas conductas referidas al tratamiento y acceso a la información.

Es imperativo apostar a una cultura de seguridad que debe programarse de manera interna y en todos los niveles, tanto administrativos como ejecutivos, y no dejar este aspecto confiado solo a dispositivos electrónicos o a un departamento técnico especializado de seguridad informática. Se está hablando de diferentes niveles de autorización de acceso a la información.

Si se analiza el accionar humano en el tratamiento de la información, se infiere una valoración del daño o impacto generado por la fuga de la información y con ello las consecuencias de daño material o moral que devienen.

A. Asunción de riesgos

La asunción de riesgos es sustancial en la protección de los datos empresarios. Y en este sentido, el nuevo Código Civil y Comercial, san-

cionado en el 2014 en la Argentina, en su artículo 1719 señala que en la asunción de riesgo:

> La exposición voluntaria por parte de la víctima a una situación de peligro no justifica el hecho dañoso ni exime de responsabilidad a menos que, por las circunstancias del caso, ella pueda calificarse como un hecho del damnificado que interrumpe total o parcialmente el nexo causal.

Se continuó con el mismo sentido original del principio *alterum non laedere*, es decir, se tiene en cuenta el deber genérico de no dañar a otro, por lo que existirá necesariamente una obligación de reparación integral del daño causado de acuerdo al impacto generado.

Para establecer los impactos negativos en el tratamiento de la información y consecuentemente poder evaluar la asunción de riesgos, más allá del cumplimiento de los marcos legales se recurrió a definir pautas como: políticas internas corporativas, identificación de personas autorizadas con o sin acceso a información, cumplimiento de cláusulas convenidas, etc.

Dentro de las políticas empresarias se entiende que es mejor prevenir en la definición de los tipos de daños que se consideran tales y sus consecuencias legales.

En este sentido se puede concluir, una vez analizada la situación en la asunción de riesgos, que la magnitud del impacto tendrá que ver con el daño que genere la indebida fuga de información desde su lugar de tratamiento o almacenamiento en la empresa, recayendo la posibilidad de la sanción y su consecuente obligación de reparación sobre quien se identifique como responsable.

B. Ingeniería social

Para adoptar medidas de seguridad con el fin de minimizar los riesgos, es necesario comprender los puntos críticos que generan mayores ocasiones en la fuga de información. Consecuente con la idea que se está exponiendo, es esencial reforzar la atención sobre el comportamiento o accionar humano, permeable a lo que llamaremos la "ingeniería social".

Se hace referencia a un concepto sin connotación sociológica alguna, focalizado en la manipulación humana o estrategia mediante la cual puede ser sometida una persona, independientemente del *hardware*, como control biométrico o *software* o *firewalls*, para obtener de ella determinada conducta esperada o deseada.

Los sujetos que trabajan o conforman la empresa como persona de existencia ideal, integrada en todos sus niveles jerárquicos, no pueden ser automatizados cual un *hardware* más, por lo que tratar de comprender quién podría dar lugar a una falla de seguridad es casi imposible.

El factor humano siempre será un punto crítico en la seguridad de la información; las

máquinas pueden ser programadas, pero no así una persona que será el eslabón más débil en la cadena de seguridad. Al decir de Cisco, la empresa estadounidense dedicada a equipos de telecomunicaciones y consultoría, "los atacantes, en lugar de centrarse en los servidores, se han percatado de que suele ser más sencillo atacar a los usuarios en el terreno del navegador y el correo electrónico" (2015, p. 18).

De hecho, en una encuesta realizada por Nuix (2015), firma australiana de investigación y consultoría sobre ciberseguridad, entre otros, se llegó a la conclusión que un porcentaje superior al 90 % de los encuestados considera como principal problema, a la hora de la protección de los datos, el comportamiento humano, recalcando la necesidad de concientización de los empleados de las empresas.

Si bien puede resultar dificultoso detectar estos casos, el hecho de conocer e interesarse en el recurso humano de una organización haría posible prevenir ciertos riesgos generadores de diferentes cuantías de daño.

Se podrían tomar medidas concretas y definir un plan de acción de prevención, aunque siempre habrá un margen de error que quedará abierto, porque donde hay tecnología hay posibilidad de fallas en el manejo de esta. Burdamente se puede figurar la escena con un muro y una puerta: desde el momento que se abre una puerta por razones de utilidad, por más seguridad que se le coloque siempre existirá la posibilidad de abrirla, pero un correcto tratamiento en el control de ese riesgo minimizará cualquier impacto generador de graves daños. Igual criterio aplica en la necesidad de extremar el control de la seguridad informática.

Vale decir que así como en la sociedad industrial moderna una variable negativa era la distribución de la riqueza, en la sociedad del conocimiento el problema es la distribución de los riesgos, y en eso justamente se focaliza la ingeniería social.

1. Casos ejemplificadores

> El concepto de ingeniería social es de larga data, tanto que puede ejemplificarse con la historia del caballo de Troya, narrada por el poeta griego Homero en *La Odisea* (siglo VIII a. C.). Cuenta que los antiguos helenos, para sortear la muralla infranqueable que protegía la ciudad de Troya, mediante manipulación psicológica lograron hacer creer al enemigo que el caballo de madera en cuyo interior se escondían los guerreros no era más que un trofeo de guerra, consiguiendo así entrar a la ciudad y cumplir su objetivo, con la colaboración de sus propias víctimas.

Ya en tiempos actuales se pueden mencionar ejemplos como el del Banco JP Morgan Chase, del que en el año 2014 se supo, a través de diferentes medios de difusión como el *New York Times* y *Bloomberg News,* que su cadena de bancos, entre otras entidades financieras de los Estados Unidos, había sido víctima de piratas internacionales que atacaron ciber-

néticamente, provocando la pérdida de datos sensibles de aproximadamente 83 millones de cuentas bancarias, la fuga y apropiación indebida de información y variaciones en el precio de acciones del mercado bursátil, generando una serie de acciones ilegales. Según afirmara el fiscal de la causa, se produjo una impactante violación de la información en estas empresas, en cuanto a su alcance y tamaño.

Otro caso de inseguridad de la información, manejado con estrategias de ingeniería social, lo dio a conocer Brian Krebs públicamente a través de su blog KrebsonSecurity (2013), donde se refiere a informes sobre ciberdelincuencia y seguridad en internet. En cifras, luego de un ataque entre los años 2013 y 2014, hizo saber que se comprometieron 1.200 millones de contraseñas y direcciones de correo electrónico en el mundo, con lo que se permitía conectarse a unos 420.000 portales de internet. Grandes sistemas fueron perjudicados, entre ellos Adobe Systems, incidiendo sobre millones de personas. La información, según especialistas como Angulo (2016), era ofrecida por *hackers* rusos dispuestos a cederla al mejor postor, contra un pago prácticamente insignificante. Se llegaron a ofrecer 57 millones de cuentas con dominio pertenecientes a Rusia, 40 millones de cuentas pertenecientes a Yahoo, 33 millones pertenecientes a Microsoft y 24 millones pertenecientes al dominio de Gmail.

Asimismo tuvo fuerte repercusión en la opinión pública, dentro del ámbito del "dato personal", el caso de Ashley Madison, el cual demuestra el fuerte impacto en la gestión de riesgo del manejo de la información. Según Albors (2015), este conocido caso de hackeo fue sufrido en agosto de 2015 por el portal Ashley Madison, cuya empresa matriz es Avid Life Media, con sede en Toronto, Canadá. El web service mencionado se dedica a realizar citas extramatrimoniales y se identifica con el eslogan "la vida es corta, busca un amante". Cuenta con usuarios de 46 países y opera desde el 2001. Un grupo autodenominado Impact Team acusó al portal de manejo de información engañosa e hizo saber que su demanda de cerrar el portal no fue oída. Se planteó una postura ética, tema que excede el presente trabajo. La empresa ofrecía borrar los datos de los usuarios que quisieran abandonar la base de datos, contra un pago. Los ciberpiratas dejaron demostrado que esto no se cumplía, cuando hicieron públicas las listas de información conteniendo entre ellas los datos de usuarios que se suponía ya no debían existir, por haber pagado para salir de ellas.

El gran impacto por la posible filtración de identidades y preferencias sexuales de millones de personas, equivalente a diez gigas de información, trajo una cantidad considerable de denuncias de chantaje y hasta dos suicidios. Un problema de seguridad que entró en crisis, reflejando el poder que tienen los piratas informáticos y el peligro que corre el tratamiento de la información que está circulando por bases de datos.

En adición a lo presentado hasta ahora, y para resaltar la importancia del debido tratamiento de la información y la necesaria disminución de

los riesgos de fuga de datos, se puede citar el mediático caso de la revelación de datos secretos de un programa de espionaje denominado PRISM. Se trató de la fuga de datos tomados a ciudadanos, realizada por Edward Snowden, un técnico que perteneció a la Agencia Central de Inteligencia (CIA, por sus siglas en inglés), creada en 1947 con la firma del Acta de Seguridad Nacional, por el presidente Harry S. Truman.

Pero Snowden no solo se circunscribió a ciudadanos estadounidenses, sino que reveló datos del espionaje en sistemas de información que perpetraba Estados Unidos sobre China, Rusia y la Unión Europea. Tales revelaciones salieron a la luz a través de diversos medios de información prestigiosos, como *Der Spiegel* de Alemania o el británico *The Guardian* que hizo saber sobre las escuchas telefónicas a más de 35 líderes mundiales (Márquez, 2013).

IV. LA INSEGURIDAD DE LA INFORMACIÓN

Habiéndose señalado la importancia de mantener el resguardo de la información, se pasa a identificar algunas de las causas genéricas que implican un serio desafío a este objetivo.

Ante el riesgo de pérdida de control sobre la información disponible en los bancos de datos, se compromete el tratamiento aplicado a esta por los responsables del manejo de datos de terceros. No debe escapar a la atención la protección otorgada a datos dispuestos en la *nube*. Lo último expresado refiere a grandes gigas de datos almacenados en forma gratuita u onerosa, que recogen información en las redes.

Se plantean cuestiones sobre la pérdida de control de los datos, como: ¿es infundado este temor?, ¿solo se trata de una percepción?, ¿sería cuestión de algún malware?, entendido este último como aquel software malicioso que se introduce en nuestros equipos tomando control bajo diversas maneras (virus, *worm, spyware, bootnet*, etc.).

Se indagó acerca de pautas a tener en cuenta para la prevención y evitar el robo, secuestro o algún otro tipo de manejo inescrupuloso de la información. Así, resultó notoria la gran oferta de anuncios dirigidos a sitios web no deseados, con publicidad que reporta ciertos ingresos, obtención fraudulenta de datos financieros, intervenciones a computadoras y usuarios mediante la modalidad conocida como *zombi*, refriéndose a aquellas capturadas por *hacker*s o virus que responden al mismo objetivo de atacar maliciosamente otros sistemas, fraudes, etc. Concluyendo en situaciones que incluso pueden provocar degradación del servicio, es decir, intensifican el ataque en momentos determinados, llegando a provocar un colapso que puede dejar fuera de actividad el sistema atacado.

Parecería, pues, que no se trata de solo percepción. De facto, la empresa Sophos, especialista en ciberseguridad, recibe diariamente solo un tercio de denuncias sobre los posibles virus existentes.

Lo que se expuso guía a la pregunta, ¿cómo se entra en contacto con tales virus?

Es conocido para el usuario en general que los programas maliciosos que atacan a los sistemas en general entran por páginas web visitadas, bajando archivos seleccionados por el propio usuario, o incluidos en otros programas que se pretenden descargar de las redes a través de archivos *peer to peer*, etc. Y a lo que se expuso se le suma la advertencia de necesaria protección para este tipo de malware; en general se avisa para que no abran archivos que vienen en mensajes de desconocidos, o que no se usen contraseñas débiles, o que se incorporen efectivos antivirus, o que no se utilicen sistemas wifi ajenos para manejar datos sensibles, etc., etc., ¿no será que debemos replantear el rol de la *ingeniería social* precisamente tanto como cuando se focaliza el rol de la *ingeniería informática*?

Se podría ir concluyendo que no se debe atribuir la fuga de información solo y principalmente a las *fallas informáticas*, como comúnmente es presumido, e ir poniendo atención al comportamiento social frente al manejo de la tecnología como vía de tratamiento de la información.

V. CAUSALES POSIBLES DE FUGA DE INFORMACIÓN O DATOS

Como resultado del punto anterior expuesto, a continuación se presentan posibles factores que darían lugar a fuga de información, siguiendo un orden de mayor a menor frecuencia en su implementación:

1) negligencia o impericia en el manejo de la seguridad de la información. Las estadísticas señalan que gran parte de la fuga de información en empresas y organismos se produce a través de los propios empleados. Producto de negligencia o impericia, entendiendo este concepto de una manera más amplia que lo estrictamente técnico informático. Por ejemplo, el correo electrónico sin cifrar, o el envío de un correo a una dirección equivocada o el almacenamiento de archivos en servicios basados en la *nube*, como podría ser en Dropbox, Gmail, etc.;

2) ataques internos. Abarca a empleados infieles quienes actúan motivados por represalia, venganza, conciencia cívica, robo de información y otras causas de tipo económico;

3) delincuentes informáticos, en mucha menor frecuencia que las anteriores. Existen técnicas capaces de robar información de dispositivos no conectados que operan de diversos modos, por ejemplo, a través de interceptar la radiofrecuencia que emiten todos los dispositivos electrónicos, desde impresoras hasta escáneres, para acceder a redes aisladas a través de espionaje electromagnético, láser, radio o el calor, para mencionar solo algunos.

De acuerdo con Sánchez (2013), según un estudio de Kaspersky Lab, proveedor ruso de

seguridad informática, casi la mitad de las empresas españolas han sufrido en alguna ocasión un robo atribuido al negligente accionar del comportamiento de sus empleados. El 50 % de las empresas españolas ha restringido o prohibido el uso de servicios de intercambio de archivos. El 47 % ha impuesto reglas para regular la conexión de dispositivos externos en los equipos corporativos.

Es decir, se infiere la existencia de controles insuficientes en materia de almacenamiento y comunicación de la información corporativa, y con ello mayor probabilidad de que un empleado *provoque fugas de datos que de infectar su equipo mediante el acceso a redes sociales.*

VI. SEGURIDAD INFORMÁTICA Y GESTIÓN DE RIESGO

A. La empresa

Por lo anteriormente expuesto deviene imprescindible que se desarrollen estos conceptos, especialmente para aquellos que no pertenecen al ámbito técnico informático.

La tecnología informática, y en particular la seguridad informática, son desde la óptica de un lego, un proceso complejo que está fuera del alcance de todo profesional no especializado.

Si nos enfocamos en el punto de vista de la *empresa*, muchas organizaciones entienden que la seguridad informática, por similitud, es una especialización del área de sistemas de información. Sin embargo, en el presente trabajo no se comparte esta visión, dado que la seguridad de la información requiere de la participación, compromiso y responsabilidad de todas las áreas de la organización. Por lo general existe una división interna de las áreas de administración de infraestructura, soporte técnico y de desarrollo de aplicaciones.

Se está comprendiendo un cambio de paradigma sobre los nuevos comportamientos sociales. Igualmente se observa una transición desde una estructura con puntos de acceso con el exterior, controlados, a otra donde existen posibilidades de teletrabajo. Desde el exterior se accede al interior de la empresa y más aún, cuando los dispositivos personales sean teléfonos móviles inteligentes, tabletas o notebooks que están fuera de la administración centralizada de la organización por motivos obvios.

En el caso de desarrollo de aplicaciones y seguridad, el tema se torna más complejo. Existe una porción importante de las áreas de sistemas ateniéndose al cumplimento de normativas de seguridad, algunas internacionales como la ISO 27000, que enmarca la gestión de seguridad de la información usada por las organizaciones, sean públicas o privadas, y de diferentes dimensiones estructurales, cuyo objetivo es mejorar prácticas o regular actividades de acuerdo a diferentes secciones de trabajo.

La detección de vulnerabilidades de seguridad es compleja. Además, se debe tener en cuenta

que el personal técnico afectado por el desarrollo de aplicaciones no cuenta generalmente con capacitación apropiada en este aspecto. Se observa que no se presenta una oferta de calidad relativa a capacitación de profesionales en lo que hace a la seguridad. No solo en lo relativo a verificación de vulnerabilidades, sino también a la producción de software seguro. Es también entendible, dado que esta capacidad no es una exigencia curricular para los empleados ni tampoco se incluyen dentro del programa de capacitación laboral. Así se demuestra la desconexión que existe entre las actividades propias de la infraestructura tecnológica y el desarrollo de sistemas.

Algunas de estas herramientas jurídicas podrían tenerse en cuenta desde el punto de vista preventivo; para el caso de las empresas: 1) Contar con un Manual de gobierno corporativo, donde se trate la protección de datos, teniendo en cuenta los principios de buena fe, compromiso y lealtad. 2) Tener el control sobre el personal de la empresa, desde su selección y contratación hasta su estado de satisfacción en ella. 3) Al momento de la contratación, incluir cláusulas en los contratos donde queden aclarados los parámetros exigidos en cuanto a la seguridad de la información. 4) Disponer de un Manual de uso de herramientas informáticas, que contenga protocolos jurídicos de seguridad, cláusulas de responsabilidad en el tratamiento de la información y el uso de las herramientas. 5) Aplicación de los estándares de seguridad, como la norma ISO 27000.

B. Usuario final

Como contrapartida de la empresa se examina asimismo el punto de vista del *usuario final*. La problemática sobre seguridad requiere de un proceso de profunda concientización. Un usuario entiende la necesidad de mantener en secreto el acceso a sus sitios personales, correo electrónico, banca electrónica, etc. Sin embargo, mantener el secreto de sus claves de acceso a los datos de la organización es de aplicación un tanto más laxa.

Se tipifican conductas en circunstancias como cuando ante la ausencia eventual por enfermedad o licencia de alguien, no se tiene ningún tipo de inconveniente en divulgar su clave a un compañero o superior que requiera acceder a datos tutelados. Esto es un problema de administración de seguridad, dado que un superior debería poder acceder a los recursos de los subordinados en forma irrestricta. Única forma de identificar quién y en qué momento accedió a determinados datos.

A través de la investigación realizada se señala que los métodos de autenticación aplicados en el usuario consisten en la verificación de combinar tres factores: algo que *conozco,* por ejemplo, una clave; algo que *tengo,* el uso de una credencial; y algo que *soy*, referido a un aspecto biométrico del individuo, por lo general pasivo, como pueden ser las huellas dactilares, el iris, el rostro, etc., y no dinámico, como sería la forma de tipeo, cadencia de la voz, etc.

No se entendería comprometer la seguridad de una organización tal, solo mediante la divulgación o el resguardo indebido de una clave por parte del usuario. Tales conductas podrían asegurarse, evitándose un eventual perjuicio irreparable.

Este tipo de comportamiento observa diferentes matices que interesa desglosar para su mayor análisis:

1) El sistema pide cambio de clave en forma periódica al usuario. ¿Se trata de un método de oscuridad, con lo cual se refiere a lo psicológico y no a la seguridad tecnológica? Se intenta mediante este método asegurar la conservación de la clave secreta, ante el temor de que el usuario la divulgue o le sea extraída, concretándose un acceso no autorizado al sistema.

   Por esta razón, el usuario es obligado a recordar todas y cada una de las múltiples claves para los diferentes accesos que disponga, como podría ser banca electrónica, redes sociales, correos electrónicos, accesos laborales, sitios de interés, tarjetas de crédito, etc., por nombrar algunos de los más frecuentes. Dado que la memoria humana tiene límites específicos que varían de individuo a individuo, es común que los usuarios concluyan que la mejor práctica consiste en anotar las claves en un papel a modo de ayuda memoria, lo cual viola todo tipo de confidencialidad, o que utilicen una sola y simple clave para absolutamente todos sus accesos. Alguno tal vez piense que mantener al resguardo ese papel es suficiente; sin embargo, de acuerdo a lo indicado por el matemático e ingeniero eléctrico del Instituto de Tecnología de Massachusetts, Claude Shannon,[1] este sería un método de oscuridad y no de seguridad, el primero es psicológico y el segundo tecnológico. Se entendería como útil pero no resulta eficaz. Un método alternativo es utilizar algún sistema de administración de contraseñas, local o WEB, los cuales son de dudosa confidencialidad.

2) No existe una forma clara de detener el robo de claves. Intervienen diversos métodos para "robar" una clave. Una de ellas es mediante fraudes conocidos como *phishing,* en los que el usuario es inducido a utilizar su clave en un portal que se asemeja al de la organización. Otro de ellos es mediante el uso de *key loggers*, muy comunes en las terminales públicas donde se pueden registrar los tipeos de los usuarios.

   Este tipo de engaños hacen que el robo de las claves sea habitual, originándose los daños consecuentes. Lamentablemente, las organizaciones que han sido víctimas de estas prácticas no publican sus estadísticas, dado que supondría un descrédito en los clientes.

1. A quien le interese ampliar sobre este punto se le recomienda el material del especialista en criptografía, seguridad de las informaciones y fundador de teorías matemáticas relacionadas con la información de los datos.

Se suele aumentar la seguridad a través del uso de *tarjetas de coordenadas* que incorporan un segundo método: el *algo que tengo,* al que se aludió antes, aunque requiere de la posesión de este documento. Existiendo la posibilidad de "robar" una clave, sería normal que el usuario negara un determinado acceso, ya sea robo por descuido o simplemente un intento de acceso indebido, y que no hubiese forma de demostrarlo. Si bien cada transacción requiere del envío de la propia dirección de internet, lo que se denomina *ip address*, también es sabido que tal sistema de direccionamiento, al igual que una dirección postal, no es portable. Por lo cual existe una distribución geográfica global del sistema de direccionamiento, que permite establecer la zona desde donde se accede a los datos. Aunque existen formas sofisticadas de evitar este tipo de control, en una primera instancia es una contramedida que podría determinar el sitio desde donde se efectúa el ingreso.

El uso de *tarjetas de coordenadas*, al igual que el sistema de *tokens,* presenta algunas ventajas adicionales puesto que se identifica al poseedor de estos elementos. Además, su nombre de usuario y clave recordada hacen el sistema más robusto y permiten evitar el eventual repudio.

Dada la aceptación general de los teléfonos móviles inteligentes, algunos organismos gubernamentales están reemplazando el uso de *tokens* por el de una aplicación instalada en estos teléfonos, que cumple las funciones de entregar un determinado código pseudoaleatorio, para adicionar a la clave de usuario como método de desafío-respuesta, que mejora los costos de eventual reposición y programación de *tokens*. Ello, entendiendo que este sistema no supone disponer de un elemento extra, tomando en cuenta que un teléfono móvil inteligente es actualmente un dispositivo ubicuo.

Se debe recordar actualizar estas políticas con la misma frecuencia paralela al avance de la tecnología y regularlas haciendo un control exhaustivo de su aplicación.

Se podrían resumir y completar los problemas de confianza en la seguridad por oscuridad, referidos a lo psicológico, teniéndose en cuenta que:

1) los trabajadores de una entidad, a quienes se les confían los mecanismos internos de las redes de la compañía, pueden cambiar su rumbo laboral y abandonar la empresa dejando al descubierto las contraseñas o *scripts* que hasta ese momento permanecían discretamente;

2) los procesos de parches lentos ante detección de vulnerabilidades en el sistema o con efectos poco predecibles serían otros de los factores del éxito o el fracaso de un ciberataque. La dinámica en los parches rápidos y con efectos predecibles facilita el proceso resolutivo. Para lo cual se aconseja prever los sistemas de *uso de comunicación inalámbrica sin autenticación ni cifrado*. Con el auge del uso de dispositivos personales para el trabajo en las empresas, conoci-

dos por el acrónimo *BYOD (Bring your own device*), los trabajadores utilizan dispositivos propios inalámbricos y/o sin cifrado, que facilitan los ciberataques y posibilitan la entrada remota de usuarios no permitidos a las redes de la compañía. El personal entiende que la responsabilidad en la seguridad corresponde a la empresa, mientras la empresa no interpreta riesgos en el uso laboral de la tecnología personal;

3) existen mecanismos deficientes para el aislamiento de redes y el control del tráfico no permitido;

4) con la introducción de los Universal Serial Bus (USB) en las empresas, cualquier trabajador puede transportar información de una red a otra pese a estar físicamente aisladas. Actualmente, en palabras de investigadores de una firma de seguridad de Berlín, incluso se puede cargar software malicioso en los programas informáticos que brindan instrucciones *(firmware)* de los USB, a través de pequeños chips que vienen en los dispositivos con USB, que no son detectables porque a ese nivel no hay escudos de protección, incluso cualquier periférico que se desee conectar podría contener software malicioso (BBC Mundo, 2014);

5) inexistencia de herramientas que identifiquen rápido cualquier actividad sospechosa. Las empresas deben disponer de una plataforma resolutiva de incidentes, que no solo integre alertas de cientos de soluciones puntuales, sino que dé respuestas a incidentes inteligentes y automatice los procesos, permitiéndoles enfocarse en los incidentes más urgentes;

6) contraseñas débiles. La gestión deficiente de los controles de acceso puede abrir las puertas con facilidad a ataques externos;

7) utilización ineficiente del ancho de banda de red;

8) gestión deficiente de la memoria que puede derivar en *buffer overflow* o descontrol a causa de cantidades superiores a las asignadas para su tratamiento.[2] Esto constituye un fallo de programación.

Expertos en ciberseguridad estiman que la permanencia media de los atacantes, en redes corporativas antes de ser detectados, es de más de un año. Tiempo suficiente que combinado con las perspectivas nombradas anteriormente puede resultar muy preocupante.

Ya expuesta la idea de seguridad informática y gestión de riesgos se debe pensar en cómo anticiparse al riesgo o peligro de dejar expuesta la información, para poder evitar daños.

Se consideran aspectos de seguridad para resguardar el activo (*asset)*, lo cual significa cono-

2. El error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto se conoce como *buffer*. Si dicha cantidad es superior a la capacidad preasignada, los *bytes* sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original, que probablemente pertenecían a datos o código almacenados en memoria.

cer el peligro, clasificarlo y protegerse de los impactos o daños de la mejor manera posible. Se deben identificar potenciales amenazas, agresores e intenciones dañinas, ya sean directas o indirectas, para poder tomar medidas de protección adecuadas.

Entonces, desde el punto de vista jurídico, la seguridad informática apunta a la protección de la información en contra de amenazas o peligros, para evitar daños y minimizar riesgos relacionados con ella.

VII. PROTECCION DE DATOS

En la seguridad informática se deben distinguir dos objetivos de protección: 1) la seguridad de la información y 2) la protección de datos.

Hasta ahora se ha hablado del aspecto seguridad de la información, seguidamente se aborda lo relacionado con la *protección de los datos*.

Ambos (seguridad de la información y protección de los datos) forman la base y justifican la selección de los elementos de información que requieren una atención especial dentro del marco de la *seguridad informática* y su consecuente responsabilidad. No obstante, las medidas de protección aplicadas normalmente serán las mismas.

En un taller realizado en Centroamérica por una ONG europea, en el marco de una capacitación y sensibilización para la seguridad de la información, se pudo experimentar un interesante ejercicio en el que los participantes trataron de distinguir cuáles serían las cuestiones de índole confidencial y de índole pública en una relación entre un particular y una entidad bancaria, involucrándose ambas en la seguridad informática. Como resultado se concluyó que existe una percepción diferente del concepto de información confidencial.

Se dijo que la seguridad informática se ocupa de la protección de los datos mismos, teniendo en cuenta los requisitos exigidos por la ley de datos personales: confidencialidad, integridad y disponibilidad, pero especialmente debemos sumarle el requisito de *autenticidad*.

Si la seguridad debe entenderse como medida de prevención del daño que se genere sobre la información, en primer lugar se deben determinar procesos y medidas de protección que garanticen un cumplimiento adecuado, de acuerdo con el principio de neutralidad tecnológica. La referencia se establece al principio por el cual sea cual fuere la tecnología aplicada la figura tipificada no se altera.

Esencialmente ha de tenerse en cuenta el proceso que conlleva cumplir con el principio de neutralidad tecnológico para no quedar desactualizado. Este tipo de procesos es tan dinámico que implica una inversión en actualización y capacitación continua, bajo una estricta supervisión.

Se deben implementar medidas de protección preventiva suficientes. Porque la gestión de riesgo informático con resultado negativo no solo conllevará pérdidas de tipo económico,

sino también asumir responsabilidades jurídicas tanto civiles como penales, contractuales y extracontractuales.

Elaborar un plan de gestión de riesgo permitirá anticiparse a este, identificando el peligro, clasificándolo, y de esta manera efectivizar una adecuada protección de los datos y de los posibles daños ante una lesión a ellos.

Se deben involucrar todos los sectores de la organización, comprometiéndolos en lograr el objetivo de seguridad, pues la falencia de cualquiera provoca la responsabilidad solidaria y mancomunada.

Ahora bien, jurídicamente hablando, la seguridad informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Coincidentemente, se observan características propias de los datos, exigidas, al menos, en la legislación argentina, es decir, la previsibilidad de las pautas que evalúan las conductas riesgosas dentro de la sociedad del conocimiento.

VIII. SUGERENCIAS PARA LA PREVENCIÓN DE IMPACTOS GENERADOS POR DAÑOS

Observándose principalmente el ámbito corporativo, y habiéndose investigado material proporcionado por empresas que trabajan con seguridad informática,[3] para evitar las principales causas de fuga de información se sugieren los siguientes puntos: 1) Tener la suficiente información para clarificar una programación segura que no dé lugar a filtrado de datos. Para ello es importante tener una acabada valoración de los datos con que se cuenta en el activo y la forma en que se deben preservar y/o eliminar. 2) Educar y concientizar al personal sobre los impactos dañosos que generaría la falta de responsabilidad en el manejo de la información. 3) No considerar solo el área técnica como única responsable de la seguridad de la información. 4) Invertir en la actualización de la tecnología que brinde seguridad técnica, acogiéndose a la actualización permanente de las normas ISO de seguridad de la información. 7) Las áreas de recursos humanos y legal deben trabajar conjuntamente para ser claros en la política de confidencialidad de la empresa.

IX. CONCLUSIÓN

La tecnología es tan necesaria como una puerta que comunica entre ambientes, pero donde hay una puerta habrá posibilidad de violaciones al cierre del paso que se pretende con ella; simple analogía con la tecnología imprescindible en la actualidad, porque donde hay tecnología y manejo de información, si no se extreman los cuidados, puede haber fuga de datos. Depende de cómo se dé el tratamiento de los

3. Como por ejemplo ESET, quien brinda soluciones de software de seguridad proveyendo protección de última generación contra amenazas informáticas.

datos y en gran parte se resalta la responsabilidad de la *ingeniería social*.

Es innegable la necesidad de redefinir parámetros de comportamientos de conducta social como generación de riesgos, que hacen que percibamos una cierta amenaza ante el nuevo mundo tecnológico basado en la sociedad del conocimiento.

Por todo lo expuesto se entiende la necesidad de educar y concientizar el recurso humano a cargo del tratamiento de datos, y extremar protecciones tanto técnicas como legales adecuadas para su protección.

Referencias

1. Acevedo, A. y Vargas, F. (Junio 2000). Reseña de *Sociología del riesgo,* de Niklas Luhmann. *Estudios sobre las Culturas Contemporáneas*, VI(11), 149-157. Obtenido de http://www.redalyc.org/articulo.oa?id=31601109

2. Albors, J. (20 de julio de 2015). Ataque a Ashley Madison comprometería a 37 millones en citas extramatrimoniales. Obtenido de https://www.welivesecurity.com/la-es/2015/07/20/ataque-ashley-madison/

3. Angulo, S. (mayo, 2016). Un hacker ruso robó más de 273 millones de credenciales. Obtenido de http://www.enter.co/chips-bits/seguridad/un-hacker-ruso-robo-mas-de-273-millones-de-credenciales/

4. BBC Mundo. (11 de agosto de 2014). ¿Por qué los USB son tan inseguros? Obtenido de http://www.bbc.com/mundo/noticias/2014/08/140811_tecnologia_seguridad_conexion_usb_computadoras_lv

5. Beck, U. (2004). *¿Qué es la globalización? Falacias del globalismo, respuestas a la globalización*. Buenos Aires: Paidós.

6. Bortnik, S. (30 de mayo de 2011). 10 mandamientos de la seguridad de la información en la empresa. Obtenido de https://www.welivesecurity.com/la-es/2011/05/30/10-mandamientos-seguridad-empresa/

7. Council of Europe. (23 de noviembre de 2001). Convention on Cybercrime. European Treaty Series No. 185. Obtenido de http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

8. Cisco. (2015). Informe Anual de Seguridad de Cisco. Obtenido de http://www.cisco.com/c/dam/global/es_es/assets/pdf/asr_final_os_ah_es.pdf

9. Decreto Reglamentario 1558 de 2001 [Presidente de la República Argentina]. Por el cual se reglamenta la Ley de datos personales. B.O. Diciembre 3 de 2001.

10. HM Government. (2015). Information security breaches survey 2015. Obtenido de https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

11. International Organization for Standardization [ISO]. ISO 27000. Obtenido de http://iso27000.es/iso27000.html#section3b

12. Krebs, B. (3 de octubre de 2013). Adobe To Announce Source Code, Customer Data Breach. Obtenido de https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/

13. Ley 25326 de 2000 [Congreso de la República Argentina]. Por la cual se dictan medidas que reglan el tratamiento de los datos personales. BO 29.527, noviembre 2 de 2000.

14. Ley 24766 de 1996. [Congreso de la República Argentina]. Por la cual se dictan medidas sobre información y productos que estén legítimamente bajo el poder de una persona. BO 28.553, diciembre 20 de 1996.

15. Márquez, W. (2 de julio de 2013). Lo que Snowden ha revelado hasta ahora del espionaje de EE. UU. Obtenido de http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm

16. Nuix. (2015). Defending Data: Turning Cybersecurity Inside Out With Corporate Leadership Perspectives on Reshaping Our Information Protection Practices. Obtenido de https://www.nuix.com/analyst-briefs/defending-data-report-2015

17. Sánchez, J. (4 de julio de 2013). Caso Snowden: ¿se puede evitar la fuga de datos en la empresa? Obtenido de: http://www.abc.es/tecnologia/redes/20130704/abci-snowden-fuga-datos-empresas-201307031318.html#disqus_thread

18. Shannon. C. E. (jul. – oct. 1948). A Mathematical theory of Communications. *The Bell System Technical Journal*, *27*, 623-656.